10
Meldplicht datalekken

Aan de orde is de behandeling van:
- **het wetsvoorstel Wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp) (33662).**

De **voorzitter**:
Ik heet de staatssecretaris van Veiligheid en Justitie van harte welkom in de Eerste Kamer. Ik heb hem helaas nog niet persoonlijk mogen ontvangen, terwijl dat gebruikelijk is als tijdens een kabinetsperiode een nieuwe bewindspersoon aantreedt. Het is de eerste keer dat de staatssecretaris van Veiligheid en Justitie in deze functie hier aanwezig is en een wetsvoorstel verdedigt. Ik feliciteer hem nogmaals met zijn benoeming en wens hem veel wijsheid toe bij de uitoefening van zijn functie en bij het debat dat nu volgt.

De beraadslaging wordt geopend.

De heer **Franken** (CDA):
Voorzitter. Wij hebben de staatssecretaris als leden van de commissie voor I&A/JBZ en voor V&J, zoals die hier heet, al eens mogen ontmoeten, maar ik feliciteer hem namens mijn fractie graag in deze plenaire zaal met zijn benoeming en wens hem succes met de werkzaamheden die hij op zich heeft genomen.

Wat betreft het wetsvoorstel dat nu aan de orde is, onderschrijft de CDA-fractie het doel van de voorgestelde meldplicht en van andere plichten met betrekking tot datalekken of ernstige incidenten op het vlak van iedere bedrijfsvoering waarbij van elektronische gegevensverwerking sprake is. Wij zien dit doel als het vergroten van het vertrouwen van het publiek in digitale gegevensverwerking. Daarnaast moet het met behulp van de voorgestelde bepalingen mogelijk zijn om lering te trekken uit opgetreden datalekken.

Bij de voorbereiding van dit wetsvoorstel is een uitgebreid traject gevolgd met twee keer een advies van de Raad van State. Naar aanleiding daarvan zijn diverse knopen doorgehakt. Wij vinden de uitkomsten daarvan niet altijd de mooiste, maar accepteren dat er dit keer is gekozen voor bestuursrechtelijke handhaving. De toezichthouder kan zware sancties opleggen, die de voorzitter van het College bescherming persoonsgegevens weleens, niet ten onrechte, "Neelie Kroesachtige boetes" heeft genoemd. Mijn fractie is er in het algemeen geen voorstander van om aan toezichthouders zware sanctiebevoegdheden toe te kennen, maar gezien het feit dat deze bevoegdheden in de lijn liggen van wat andere toezichthouders, zoals de Autoriteit Consument & Markt, mogen doen, dat het overtreden van de norm mogelijk zeer grote schade ten gevolge heeft en er binnenkort Europese regelgeving is te verwachten waardoor dergelijke sancties in de gehele Europese Unie kunnen worden opgelegd, gaat zij met dit voorstel mee.

In het voorlopig verslag hebben wij een vijftal vragen gesteld, waarop goed uitgewerkte antwoorden zijn gekomen. Hulde daarvoor. Op een van die vragen, die met betrekking tot de "onbepaaldheid" van de door de burger in acht te nemen norm, gaan wij graag nog eens in. We weten allen dat een met behulp van sancties te handhaven norm voldoende duidelijk, voorzienbaar en kenbaar moet zijn overeenkomstig het lex certa-beginsel. Wij zijn er vooralsnog niet van overtuigd dat hiervan in het voorgestelde artikel 34a sprake is. De norm houdt immers in dat het gaat om "een inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens". Nu kan het College bescherming persoonsgegevens voor het opleggen van de hiermee samenhangende bestuurlijke boete weliswaar eerst bindende aanwijzingen geven voor het geval dat de overtreding niet opzettelijk is gepleegd, maar feit blijft dat er voor de burger onzekerheid bestaat over de vraag wanneer er precies sprake is van een normovertreding. Dit kan tot een overreactie van de burger leiden. De burger gaat dan, "better safe than sorry", bij ieder twijfelgeval maar melden of hij gaat er "gewoon" aan voorbij, zoals we bij de cookiemeldingen ook vaak zien. Dan geeft de norm aanleiding tot het tegendeel, dus tot "undercompliance". De staatssecretaris is daar optimistisch over. Hij gaat ervan uit dat de burger wel een beredeneerde overweging zal maken over de vraag of een concreet datalek dat hem ter kennis komt, onder het bereik van de meldplicht valt. Mijn fractie is van mening dat hier vooraf meer duidelijkheid over moet worden gegeven. Daarom vraagt zij de staatssecretaris om een interpretatie van in ieder geval de "aanzienlijke kans op ernstige nadelige gevolgen", zoals omschreven in artikel 34a, lid 1, die meer helderheid en houvast biedt. Wat wordt hier nu precies bedoeld?

In wet en jurisprudentie zien we bij vragen van onzekerheid onderscheid tussen "met aan zekerheid grenzende waarschijnlijkheid", de "aanmerkelijke kans", welke formulering wordt gebruikt bij voorwaardelijk opzet, of "wat er redelijkerwijs te verwachten is". Bij bewijsstandaarden worden om een mate van waarschijnlijkheid uit te drukken begrippen gebruikt zoals "aannemelijkheid", "een redelijke mate van zekerheid", dat je vooral in kortgedingvonnissen leest, of "boven redelijke twijfel verheven". Op welk niveau moeten we nu uitkomen? Met de opvatting dat iedere vage norm interpretatie behoeft, kan de staatssecretaris hier niet wegkomen. Het gaat immers om een met een punitieve sanctie te handhaven wettelijke bepaling. Wij vragen de staatssecretaris daarom, een soort interpretatieve verklaring te geven over hoe deze vage begrippen in artikel 34a moeten worden gehanteerd. De burger heeft een concreet handvat nodig. Dat ontbreekt nu ten enenmale. Wij zien het antwoord van de minister op deze vraag met belangstelling tegemoet.

Mevrouw **Ter Horst** (PvdA):
Voorzitter. Ik dank mevrouw Gerkens dat ik vóór haar mag spreken. Ook feliciteer ik de staatssecretaris namens mijn fractie. Ik wens hem veel succes.

De PvdA-fractie dankt de staatssecretaris voor de in de memorie van antwoord opgenomen reacties op haar vragen. In het voorlopig verslag heeft zij aangegeven dat zij het bieden van de mogelijkheid aan het College bescherming persoonsgegevens om een bestuurlijke boete op te leggen, positief beoordeelt. De verplichting om een overzicht bij te houden van potentiële of echt ernstige lekken, die de melder zelf aan de toezichthouder heeft gemeld, en de meldplicht zelve vindt zij een goede zaak. Wel heeft zij beargumenteerd dat het geven van een eventueel bindende aanwijzing vooraf in de meeste gevallen geïndiceerd is. Deze noodzaak wordt vooral ingegeven door de onduidelijkheid over de vraag of een datalek daadwerkelijk aan het College bescherming persoonsgegevens dan wel aan betrokkenen moet worden gemeld. Hierin schuilt naar de mening van mijn fractie de zwakte van het wetsvoorstel. Haar vragen hadden dan ook daarop betrekking. Daarom is het nu aan haar om te beoordelen of de antwoorden van de staatssecretaris haar verder hebben geholpen. Eerlijk gezegd is dat niet het geval geweest.

Het soort datalek waarvan verplicht melding wordt gemaakt, wordt in het wetsvoorstel als volgt omschreven. Ik citeer dezelfde woorden als de heer Franken: "een inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens". Zowel de term "aanzienlijk" als de term "ernstige" behoeft operationalisatie. In de memorie van antwoord hebben wij helaas niets kunnen aantreffen wat tot een nadere specificatie van deze termen leidt, anders dan de opmerking dat het College bescherming persoonsgegevens richtsnoeren gaat opstellen. Wij kennen die richtsnoeren niet, dus kunnen niet beoordelen of deze de beoordeling vergemakkelijken om wel of niet te melden. Graag vragen wij de staatssecretaris of hij ons al iets over die richtsnoeren en de omvang ervan kan meedelen en of hij die aan de Eerste Kamer wil zenden, zodra ze bekend zijn, zodat zij zich daar te zijner tijd een oordeel over kan vormen. De staatssecretaris geeft overigens in reactie op vragen van D66 wel een aantal voorbeelden van gevallen waarin wel en wanneer niet moet worden gemeld. Die heb ik natuurlijk goed bekeken, maar mijn constatering was dat de nuances voor wanneer wel of wanneer niet moet worden gemeld, zo gering zijn dat de vrees bij de Partij van de Arbeid alleen maar is toegenomen dat — ook hier mijn excuses aan de heer Franken — "better safe than sorry" de praktijk zal worden. Immers, op wel melden staat geen straf en op niet melden staat wel een straf. Wij vrezen dat dit tot een hausse aan meldingen zal leiden. De PvdA-fractie zou graag zien dat aan het College bescherming persoonsgegevens wordt gevraagd om jaarlijks over de aard en omvang van de meldingen van datalekken te rapporteren.

Tot slot. De staatssecretaris heeft in reactie op een vraag van een collega van het CDA een overzicht opgenomen van thans of binnenkort geldende meldplichten die betrekking hebben op de bedrijfsvoering in de private of publieke sector. Als ik goed geteld heb, zijn dat er elf. Er zijn dus elf meldplichten. De staatssecretaris geeft dat overzicht, waarvoor dank, maar verbindt daaraan geen conclusies. De PvdA-fractie zou graag van de staatssecretaris vernemen of hij verrast was door dit aantal. Er zit immers een nieuwe staatssecretaris. Misschien dacht hij ook: oei, dat zijn er wel erg veel! Was hij verrast door dit aantal? Meent hij dat het voor bedrijven nog doenlijk is om al deze meldplichten bij en uit elkaar te houden?

Ik sluit positief af. De overige punten die door de PvdA-fractie aan de orde zijn gesteld, zoals bestuurlijke strafbeschikking in plaats van of naast een bestuurlijke boete, strafbaarstelling in plaats van een bestuurlijke boete en de hoogte van de boete, zijn door de staatssecretaris naar grote tevredenheid beantwoord. Wij wachten gespannen op zijn beantwoording van de vragen die wij nu hebben gesteld.

☐

Mevrouw **Gerkens** (SP):
Voorzitter. Ik lever mijn inbreng mede namens de fractie van GroenLinks. Ook ik wil de nieuwe staatssecretaris welkom heten in de Eerste Kamer. Ik hoop dat ik met hem net zo goed kan samenwerken als met zijn voorganger, de heer Teeven.

Allereerst bedank ik de staatssecretaris voor de beantwoording van onze vragen. De fractie van de SP is blij met dit wetsvoorstel, dat in onze ogen veel te lang op zich heeft laten wachten. Die lange wachttijd heeft ons ook wat bevreemd: zo'n lastig onderwerp is het niet en voor de bescherming van de internetgebruiker is het van groot belang dat datalekken gemeld worden. Uit de beantwoording van de staatssecretaris mag ik voorzichtig concluderen dat ook hij vindt dat deze weg lang is geweest.

Toch wilde mijn fractie nog mondeling met de staatssecretaris hierover van gedachten wisselen. Het gaat in dit debat om de kwaliteit van de uitvoering van dit wetsvoorstel. Laten we daarvoor eerst eens kijken naar het waarom van dit wetsvoorstel. In 2007 werden door een lek bij Tel Sell de creditcardgegevens van ruim 30.000 klanten gestolen. Maanden later werd dit pas bekend. Het bedrijf had zijn klanten niet op de hoogte gesteld omdat het niet zijn verantwoordelijkheid was, zo vond het bedrijf. Dit was een van de eerste grote lekken die bekend werden. Eigenlijk is iedereen het erover eens dat wanneer er een lek is, dit gemeld dient te worden, maar over het hoe en wat verschilt mijn fractie van mening met dit kabinet.

De vertraging is hierom wel te begrijpen. Het wetsvoorstel moet uitvoerbaar zijn en het moet kunnen rekenen op draagvlak in de uitvoering. En laten we eerlijk zijn, het is momenteel voor geen enkele organisatie prettig om te melden dat er ingebroken is in het digitale systeem, laat staan om dan ook nog eens te vertellen dat er gegevens zijn gestolen. Er heerst bij velen nog een taboe op het gegeven dat inbraak mogelijk is.

Tijdens het afgelopen paasweekend werd er bij het opslagbedrijf Hatton Garden Safe Deposit 270 miljoen euro buitgemaakt. Dat was spectaculair, want dit stond bekend als een van de beste beveiligde bedrijven. Metersdik gestaald beton werd doorboord. Offline en online bestaat er dus niet zoiets als absolute veiligheid, maar het besef daarvan is nog altijd laag. Er zijn bedrijven die hun best doen om de beveiliging hoog te houden, maar er zijn er ook die beschamend met de veiligheid omgaan. Ik noemde in het verslag al de grote pensioenuitvoerder die de volledige pensioenoverdracht online aanbood, inclusief bsn, inkomen van deelnemer, inkomen van partner, adresgegevens en noem maar op, allemaal over een onbeveiligde lijn. Kinderdagverblijven gebruiken onlineformulieren voor de inschrijving met een bsn over een onbeveiligde lijn. Dan heb ik het nog niet eens over de informatie die van mij

gevraagd wordt als ik een simpele nieuwsbrief wil ontvangen of mijn gegevens achterlaat bij een webshop of op een contactformulier. Vaak zijn dat onnodige gegevens, zoals geboortedata et cetera, met daardoor extra risico op nog meer datalekken.

Ik zie drie mindsets die gewijzigd moeten worden. Allereerst is dat de mindset van de aanbieder van de dienst op het gebied van de Wet bescherming persoonsgegevens. Deze wet is nog onvoldoende in beeld bij de aanbieders. Zeker het mkb heeft hier nog een slag te maken, maar helaas ook de grotere organisaties. Ik zou hier vele voorbeelden kunnen noemen.

Ten tweede gaat het om de mindset van dezelfde aanbieders op het gebied van veiligheid. Omdat het hier om techniek gaat, vragen aanbieders nog veel te weinig expliciet naar de beveiliging. Zij gaan er namelijk vanzelfsprekend van uit dat de websitebouwer die wel in de gaten houdt, maar dat is over het algemeen niet zo. Zelfs als dit wel gebeurt, is het voor een aanbieder lastig te bepalen of de gevraagde veiligheid ook geboden wordt. Ik maak het mee dat hosts hun software op de server niet updaten. Dan denkt de aanbieder dat hij veilig is, maar blijkt dat niet zo te zijn.

Ten derde gaat het om de mindset van de gebruiker, die moet beseffen dat een lek geen onwil is van een organisatie en dat hij altijd zijn wachtwoord dient te wijzigen bij de melding van een lek, en liefst nog wat vaker. Wanneer ik echt een dienst wil afnemen, maar de beveiliging onvoldoende is, dan mail ik het bedrijf met die opmerking. Een veilig internet is ook samenwerken.

In het verslag vertelde mijn fractie over het Heartbleed-lek van afgelopen zomer en de wijze waarop de gebruiker daarover werd geïnformeerd. Zo wist ik dat mijn e-mailadres tot de hack behoorde, maar niet waar het lek zat en of ik passende maatregelen moest nemen. Er werd mij alleen geadviseerd om mijn wachtwoorden te wijzigen. Ik heb er veel, heel veel, en zou niet eens weten of ik dan alle wachtwoorden zou hebben gehad. Deze impasse leidde ertoe dat ik niets deed, een soort Catch-22. Hier raken wij een kwetsbaar punt van de uitvoering. Mijn fractie is het met de regering eens dat er alleen gewaarschuwd dient te worden als er sprake is van mogelijke diefstal van persoonlijke gegevens, maar op welke wijze dat gebeurt en wanneer daarvan precies sprake is, is onduidelijk en wordt aan de aanbieder overgelaten. Deze moet wel altijd de hack melden bij het CBP, maar het wetsvoorstel biedt geen garantie dat de aanbieder ook op de juiste wijze zijn klanten informeert. Zo werd bij het Heartbleed-lek geen adequate waarschuwing gegeven omdat dan bekend zou worden welke websites op dat moment kwetsbaar waren, maar naar ik mag aannemen is zo'n lek snel gedicht en had men de gebruikers vervolgens alsnog kunnen waarschuwen.

Het wetsvoorstel verbetert dus wel de mogelijkheden van het CBP en in zekere mate de bewustwording bij de aanbieder, maar beschermt nog veel te weinig de eindgebruiker om wie het in dit wetsvoorstel uiteindelijk te doen is. In het verslag verwijst de staatssecretaris naar een brief aan de Voorzitter van de Tweede Kamer der Staten-Generaal van 13 oktober 2014 inzake de Hold-casus. In die brief heeft de minister van Veiligheid en Justitie toegezegd dat voorts zal worden verkend "hoe de ervaringen uit deze casus geborgd kunnen worden in een te ontwikkelen structurele voorziening met de daarbij benodigde juridische waarborgen". Kan de staatssecretaris mij vertellen wanneer deze structurele voorziening en de daarbij behorende waarborgen worden ontwikkeld? Dit lijkt mij een welkome aanvulling op het wetsvoorstel. Zou een dergelijk voorstel voor het eind van dit jaar naar de Tweede Kamer gezonden kunnen worden? Graag krijg ik een reactie van de staatssecretaris.

Ik wil graag nog even terugkomen op de awareness. Het ECP is inderdaad volop met het mkb bezig om de digitale veiligheid daar te verbeteren. Ik ken het programma en dat is gedegen en succesvol, maar het bereik blijft klein. De gemiddelde aanbieder heeft echt geen flauw benul van de Wet bescherming persoonsgegevens. Voor aanbieders is het niet meer dan logisch dat ze voor de verzending van hun artikelen naw-gegevens nodig hebben. "Waarom zijn die nou zo privacygevoelig?", zo redeneren zij. Is de staatssecretaris bereid om eenmalig aan alle bedrijven en organisaties die bij de Kamer van Koophandel zijn ingeschreven, een brief te zenden waarin hij wijst op deze wet en op de Wet bescherming persoonsgegevens? Vervolgens kan hij in deze brief ook verwijzen naar het programma van ECP. Hiermee zouden we een enorm grote slag kunnen slaan. Graag verneem ik de reactie van de staatssecretaris.

Mij rest nog een klein vraagje. In de beantwoording zegt de staatssecretaris dat het aan de beoordeling van de aanbieder zelf is hoelang hij het overzicht van inbreuken moet bewaren. Hierop staat dezelfde boete als op het niet naleven van de meldplicht. Dat kan echt niet. Er staat een behoorlijke boete op het spel. Het bewaren van documenten loopt van twee jaar tot levenslang. Mijn fractie zou willen voorstellen dat in ieder geval het CBP aangeeft hoelang deze informatie bewaard dient te worden, zodat dat bij ingang van deze wet voor iedereen helder is. Ik kijk uit naar de beantwoording.

De beraadslaging wordt geschorst.

De vergadering wordt van 15.39 uur tot 15.43 uur geschorst.